IN THE UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF TENNESSEE

MANDI PHILLIPS, on behalf of Herself and all others similarly situated,	)	
Plaintiff,	)	
vs.	)	**CASE NO 3-14 1710**
MAPCO EXPRESS, INC., Owned and Operated by DELEK US HOLDINGS, INC.,	)	
Defendants.	)	

PLAINTIFF'S CLASS ACTION COMPLAINT

Plaintiff, MANDI PHILLIPS ("Plaintiff"), hereby brings this class action suit against MAPCO Express, Inc. ("MAPCO" or "Defendant Mapco"), owned and operated by DELEK US HOLDINGS, INC. and DELEK US HOLDINGS, INC. ("DELEK" or "Defendant Delek"), on behalf of herself and other similarly situated individuals. Plaintiff makes the following allegations based upon the investigation undertaken by Plaintiff's counsel, which included, inter alia, information from Plaintiff, review and analysis of Defendants' website and press release, and various news articles and public reports.

NATURE OF THIS ACTION

1. Plaintiff brings this class action suit on her own behalf and on behalf of all other persons or entities in the United States against MAPCO and DELEK US HOLDINGS, INC. to redress MAPCO's and DELEK'S failure to adequately safeguard certain credit card and debit

card information and related data. More specifically, this action arises from MAPCO's and DELEK's failure to maintain adequate computer data security of customer credit and debit card data, which was accessed and taken by a computer "hacker." As a result of MAPCO's and DELEK's wrongful actions, customer information was taken from MAPCO's and DELEK's computer network that handles a wide range of financial information for millions of transactions, including credit cards and debit cards linked to checking accounts. Because of MAPCO's and DELEK's actions, many of its customers have had their personal financial information or what is known as their personal customer account information ("PCAI") compromised, have had their privacy rights violated, have been exposed to and suffered the risk of fraud and identity theft and the threat of fraud and identity theft, have been the victims of fraud, and have otherwise suffered damages.

JURISDICTION AND VENUE

2. Jurisdiction of this Court is invoked pursuant to 28 U.S.C.A 1332(d), as the matter in controversy exceeds $5 million, Plaintiff has diverse citizenship from Defendants MAPCO and DELEK, and there are more than 100 class Members. The Court also has subject matter jurisdiction over Plaintiff's FCRA claims pursuant to 27 U.S.C. § 1331 because it is a federal question of law. This Court has personal jurisdiction over Defendants because at all relevant times, Defendants have conducted business in the Middle District of Tennessee.

3. Venue properly lies in this District pursuant to 28 U.S.C. §1391(a)(2), since the cause of action arose in this District, and the unlawful conduct of Defendant, out of which the cause of action arose, took place in this District.

PARTIES

4. Plaintiff MANDI PHILLIPS resides in Childersburg, Alabama. Plaintiff made debit card purchases at Defendants' retail facility. Plaintiff's account information was provided to Defendant via her debit card transaction and Plaintiff's debit card data was subject to release to unauthorized and unknown individuals from MAPCO's and DELEK's computer system. On or around July 14, 2013, Plaintiff attempted to use her card in Oxford, Alabama and her card was declined. She later attempted to use the same card again in Childersburg and was declined two more times. On July 16, 2013, Heritage South Credit Union notified Plaintiff that her card had been compromised. Plaintiff had to drive to the Sylacauga branch of Heritage South Credit Union to get a new card. Plaintiff was unable to use the funds that were in her account for approximately thirteen days. Plaintiff has been damaged as a result.

5. Plaintiff shopped at Defendants retail locations again on December 9, 2013. Plaintiff's account information was provided to Defendant via her debit card transaction and Plaintiff's debit card data was subject to release to unauthorized and unknown individuals from MAPCO's and DELEK's computer system. On December 9, 2013 at 4:49 p.m., Plaintiff was notified by the Alabama Telco Union Fraud Department that her card had been compromised again. Plaintiff has been damaged as a result.

6. Defendant MAPCO Express, Inc. is a Tennessee corporation owned and operated by DELEK US HOLDINGS, INC., with its headquarters at 7102 Commerce Way, Brentwood, Tennessee 37027. MAPCO operates convenient store or "c-store" chains in Tennessee, Mississippi, and throughout the southeastern United States. As noted on its website and related materials, MAPCO Express, Inc., is a wholly-owned subsidiary of Delek US Holdings, Inc. with

company headquarters in Brentwood, Tennessee. MAPCO operates convenience stores in at least seven states under the MAPCO Express®, MAPCO Mart®, East Coast®, Discount Food Mart™, Fast Food and Fuel™, Delta Express®, and Favorite Markets® brand names. MAPCO is one of the largest company-operated convenience store chains in the United States, and one of the leading "c-store" operators of the southeast. More than half of the retail segment's store locations are in Tennessee. MAPCO owns the real estate of more than half of the stores it operates.

7. Defendant DELEK US HOLDINGS, INC. is a Tennessee corporation and the parent company of MAPCO Express, Inc., with its headquarters at 7102 Commerce Way, Brentwood, Tennessee 37027.

OPERATIVE FACTS

8. MAPCO and DELEK US HOLDINGS, INC. operate retail fuel and convenience stores in the United States. It offers fountain drinks, coffee, sandwiches, snack items, beverages, beef burgers, cheese steaks, chicken, and ice creams as well as fuel and related services. The company was incorporated in 2001 and is headquartered in Brentwood, Tennessee. MAPCO operates as a subsidiary of Delek US Holdings, Inc.

9. On May 6, 2013, MAPCO first publicly announced that it has been hit by a wide-reaching security breach that may leave thousands of customers exposed to fraud and identify theft from transactions that date back to March 2013. MAPCO's press release stated, in relevant part:

> Convenience store operator MAPCO Express, Inc. ("MAPCO") has experienced a security breach by third-party hackers that may have compromised the credit/debit card information of certain MAPCO customers. MAPCO operates convenience stores in Tennessee, northern

> and central Alabama, northern Georgia, Arkansas, Virginia, southern Kentucky and northern Mississippi under the MAPCO Express®, MAPCO Mart®, East Coast®, Discount Food Mart™, Fast Food and Fuel™, Delta Express®, and Favorite Markets® brand names.
>
> . . .

As noted in the release, through its investigation, MAPCO has learned the following with respect to the intrusion:

- The incident involves credit/debit card payments for transactions at MAPCO locations between March 19-25, April 14-15 and April 20-21.
- MAPCO is notifying potentially affected customers because information may have been stolen that can be used to initiate fraudulent credit and debit card transactions.
- Upon discovering the issue, MAPCO took immediate steps to investigate the incident and further strengthened the security of its payment card processing systems to block future information security attacks.
- MAPCO is working with nationally recognized computer forensics investigation firms and the payment card associations to determine what happened and the extent of the information that may have been compromised.
- MAPCO is also working with law enforcement, including the FBI's Joint Cyber Crime Task Force, to identify the perpetrator.

10. MAPCO's press release also stated that after the security breach occurred, the Company "further strengthened the security of its payment card processing systems." The Company did not specify the nature of the improvements.

11. U.S. retailers, including MAPCO and DELEK, are required to follow stringent card-industry rules. The rules that cover transactions on card branded with logos from Visa, MasterCard International, Inc., American Express Co. and Discovery Financial Services, and others, require merchants to validate a series of security measures, such as the establishment of

firewalls to protect databases. Among other things, merchants are prohibited from storing unprotected cardholder information.

12. Plaintiff, Mandi Phillips, suffered at least one unauthorized transaction to her account at the Alabama Telco Credit Union. The transaction took place on December 9, 2013 at Banco Popular in New York. Plaintiff also suffered additional unauthorized attempts on her account on December 9, 2013 in the state of New York. These unauthorized attempts took place at Amherst for $200.00 and at Banco Popular for $99. The unauthorized transactions occurred on the same debit or credit card that Plaintiff used at defendants retail locations at the dates noted. Plaintiff was not in the state of New York when the attempts took place and did not authorize anyone else to use her card. All of these charges occurred after Plaintiff shopped at defendants retail locations on the noted dates. Furthermore, Plaintiff has suffered the threat of additional unauthorized transactions and has incurred expense and the lost of time related to changing cards and accounts because of the Defendants' breach.

13. The security breach at MAPCO is currently being investigated by the Federal Bureau of Investigation, and other law enforcement agencies.

14. Plaintiff, Mandi Phillips, made purchases at MAPCO Express, Inc. facilities during the relevant time period and did so because she was led to believe that the Defendants would not allow her personal and private information to be disseminated to other unknown persons or entities.

CLASS ACTION ALLEGATIONS

15. Plaintiff brings this class action, pursuant to Federal Rule of Civil Procedure 23(a) and (b)(3), on behalf of herself and all others similarly situated, consisting of all persons or entities in the United States who have had personal or financial data stolen from MAPCO's and DELEK's computer network and who were damaged thereby (the "Class"). The Class does not include MAPCO and DELEK, or its officers, directors, agents, or employees.

16. The Class consists of hundreds and possibly thousands of customers of MAPCO and its subsidiaries located throughout Alabama and the southeast United States, and DELEK. While the exact number of Class Members and the identities of individual Class Members are unknown at this time, and can only be ascertained through appropriate discovery, based on the fact that thousands of customer accounts have already been affected, the Class is so numerous that joinder of all Class Members is impracticable.

17. Defendants' conduct affected all Class Members in exactly the same way. Defendants' conduct in failing to properly safeguard its customers' personal and financial data and in failing to notify customers of the security breach as soon as practical after the breach was discovered is completely uniform among the Class.

18. Questions of law and fact common to all Class Members predominate over any questions affecting only individual members. Such questions of law and fact common to the Class include but are not limited to:

a. Whether or not Defendant acted wrongfully by failing to properly safeguard its customers' financial data;

b. Whether or not Defendant failed to notify Class Members of the security breach as soon as practical after the breach was discovered;

c. Whether or not Plaintiff and the Class have been damaged, and if so, what is the appropriate relief as to each member of the Class.

d. Whether Defendants violated FCRA by failing to properly secure and transport Plaintiff's and Class Members' PCAI;

e. Whether Defendants violated FCRA by failing to encrypt Plaintiff's and Class Members' PCAI in accordance with federal standards;

f. Whether Defendants willfully, recklessly and/or negligently failed to maintain and/or execute reasonable procedures designed to prevent unauthorized access to Plaintiff's and Class Members' PCAI;

g. Whether Defendants was negligent in storing Plaintiff's and Class Members' PCAI;

h. Whether Defendants owed a duty to Plaintiff and Class Members to exercise reasonable care in protecting and securing their PCAI;

i. Whether Defendant breached a duty to exercise reasonable care in failing to protect and secure Plaintiff's and Class Members' PCAI;

j. Whether Defendants was negligent in failing to secure Plaintiff's and Class Members' PCAI;

k. Whether by publicly disclosing Plaintiff's and Class Members' PCAI without authorization, Defendants invaded Plaintiff's and Class Members' privacy; and

l. Whether Plaintiff and Class Members sustained damages as a result of Defendants' failure to secure and protect their PCAI.

19. Plaintiff's claims, as described herein, are typical of the claims of all Class Members, as the claims of Plaintiff and all Class Members arise from the same set of facts regarding Defendants' failure to protect Class Members' financial data. Plaintiff maintains no interests that are antagonistic to the interests of other Class Members.

20. Plaintiff is committed to the vigorous prosecution of this action and has retained competent counsel experienced in the prosecution of class actions of this type. Accordingly, Plaintiff is an adequate representative of the Class and will fairly and adequately protect the interests of the Class.

21. This class action is a fair and efficient method of adjudicating the claims of Plaintiff and the Class for the following reasons:

a. Common questions of law and fact predominate over any question affecting any individual Class member;

b. The prosecution of separate actions by individual members of the Class would likely create a risk of inconsistent or varying adjudications with respect to individual members of the Class thereby establishing incompatible standards of conduct for Defendant or would allow some Class Members' claims to adversely affect other Class Members' ability to protect their interests;

c. Plaintiff is not aware of any other litigation of these issues ongoing in this State or elsewhere brought by a nationwide class of consumers of MAPCO and DELEK;

d. This forum is appropriate for litigation of this action since the cause of action arose in this District;

e. Plaintiff anticipates no difficulty in the management of this litigation as a class action; and

f. The Class is readily definable, and prosecution as a class action will eliminate the possibility of repetitious litigation, while also providing redress for claims that may be too small to support the expense of individual, complex litigation.

22. For these reasons, a class action is superior to other available methods for the fair and efficient adjudication of this controversy.

COUNT I

INTENTIONAL VIOLATIONS OF THE FAIR CREDIT REPORTING ACT ("FCRA")

23. Plaintiff re-alleges the above paragraphs as if fully set forth herein.

24. This is a claim for violation of the FCRA. *See, generally,* 15 U.S.C. § 1681 *et seq.*

25. FCRA requires the proper disposal or transfer of Consumer Information. *See* 15 U.S.C. §1681w and 16 C.F.R. § 682 *et seq.*

26. In compliance with FCRA, the Federal trade Commission ("FTC") codified 16 C.F.R. § 682 *et seq.*, which regulates the responsibility of companies and individuals who possess Consumer Information. The purpose of the section is to reduce the risk of consumer fraud and related harms, including identity theft, created by the improper disposal of consumer information. *See* 16 C.F.R. 682.2(a).

27. "Consumer Information" is defined as "any record about an individual, whether in paper, electronic, or other form that is a consumer report or derived from a consumer report.

Consumer Information also means a compilation of such records. Consumer Information does not include information that does not identify individuals, such as aggregate information or blind data." 16 C.F.R. § 682.1(b).

28. The Personal Financial Information stolen was Consumer Information as defined by 16 C.F.R. 682.1 and FCRA.

29. 16 C.F.R. 682.3 requires that "[a]ny person who maintains or otherwise possesses consumer information for a business purpose must properly dispose of such information by taking reasonable measures to protect against unauthorized access to or use of the information in connections with its disposal."

30. "Disposal" is defined as "the…transfer of any medium, including computer equipment, upon which consumer information is stored."

31. Under FCRA, a "consumer report" means any written, oral or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used in whole or in part for the purpose of serving as a factor in establishing the consumers' eligibility for credit or insurance to be used primarily for personal, family, or household purposes; employment purposes; or any other purpose authorized under 15 U.S.C. § 1681b. *See* 15 U.S.C. § 1681a(d)(1).

32. "Consumer reporting agency" means any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing Consumer Reports to third parties, and which uses any means or facility of

interstate commerce for the purpose of preparing or furnishing Consumer Reports. 15 U.S.C. § 1681a(f).

33. Defendants are a Consumer Reporting Agency and/or possesses and transfers information derived from a consumer report.

34. Plaintiff and other Class Members are "consumers" or "persons," as defined and contemplated under FCRA. *See* 15 U.S.C. § 1681a(b) and (c).

35. Defendant was required under FCRA to take reasonable measures to protect against unauthorized access while transferring Consumer Information. *See* 16 C.F.R. § 682.3.

36. In conscious disregard of the rights of the Plaintiff and Class Members, Defendant deliberately and/or recklessly did not maintain reasonable procedures designed to protect against unauthorized access while transferring or storing the Personal Financial Information.

37. As described above, Defendants' deliberate and/or reckless conduct allowed third parties to steal, or otherwise access, the Personal Information without Plaintiff's or Class Members' consent and for no permissible purpose under FCRA.

38. Defendants' conduct violated FCRA, and Plaintiff and Class Members have been damaged by Defendants' deliberate and/or reckless actions.

39. As a result of Defendants' conduct, Plaintiff and Class Members are entitled to actual damages sustained and statutory damages of not less than $ 100.00 and not more than $1,000.00, as well as the costs and attorneys' fees in bringing this action. 15 U.S.C. § 1681n.

COUNT II

NEGLIGENT VIOLATIONS OF THE FCRA

40. Plaintiff re-alleges the above paragraphs as if full set forth herein.

41. This is a claim for negligent violation of the FCRA.

42. FCRA requires the proper disposal or transfer of Consumer Information. *See* 15 U.S.C. §1681w and 16 C.F.R. § 682, *et seq*.

43. In compliance with FCRA, the Federal trade Commission ("FTC") codified 16 C.F.R. § 682 *et seq*., which regulates the responsibility of companies and individuals who possess Consumer Information. The purpose of the section is to reduce the risk of consumer fraud and related harms, including identity theft, created by the improper disposal of consumer information. *See* 16 C.F.R. 682.2(a).

44. "Consumer Information" is defined as "any record about an individual, whether in paper, electronic, or other form that is a consumer report or derived from a consumer report. Consumer Information also means a compilation of such records. Consumer Information does not include information that does not identify individuals, such as aggregate information or blind data." 16 C.F.R. § 682.1(b).

45. The Personal Financial Information stolen was Consumer Information as defined by 16 C.F.R. 682.1 and FCRA.

46. 16 C.F.R. 682.3 requires that "[a]ny person who maintains or otherwise possesses consumer information for a business purpose must properly dispose of such information by taking reasonable measures to protect against unauthorized access to or use of the information in connections with its disposal."

47. "Disposal" is defined as "the…transfer of any medium, including computer equipment, upon which consumer information is stored."

48. Under FCRA, a "consumer report" means any written, oral or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used in whole or in part for the purpose of serving as a factor in establishing the consumers' eligibility for credit or insurance to be used primarily for personal, family, or household purposes; employment purposes; or any other purpose authorized under 15 U.S.C. § 1681b. *See* 15 U.S.C. § 1681a(d)(1).

49. "Consumer reporting agency" means any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing Consumer Reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing Consumer Reports. 15 U.S.C. § 1681a(f).

50. Defendants are a Consumer Reporting Agency and/or possesses and transfers information derived from a consumer report.

51. Plaintiff and other Class Members are "consumers" or "persons," as defined and construed under FCRA. *See* 15 U.S.C. § 1681a(b) and (c).

52. Defendant was required under FCRA to take reasonable measures to protect against unauthorized access while transferring Consumer Information. *See* 16 C.F.R. § 682.3.

53. Defendant was negligent in failing to maintain reasonable procedures designed to protect against the unauthorized access while transferring the Personal Financial Information.

54. As described above, Defendants' conduct allowed third parties to steal, or otherwise access, the Personal Information without Plaintiff's or Class Members' consent and for no permissible purpose under FCRA.

55. Defendants' conduct violated FCRA, and Plaintiff and Class Members have been damaged by Defendants' negligent actions.

56. As a result of Defendants' conduct, Plaintiff and Class Members are entitled to actual damages to be proven at trial, as well as the costs and the costs and attorneys' fees in bringing this action. 15 U.S.C. § 1681o.

COUNT III

INVASION OF PRIVACY BY PUBLIC DISCLOSURE OF PRIVATE FACTS

57. The preceding factual statements and allegations are incorporated herein by reference.

58. Plaintiff's and Class Members' PCAI were (and continue to be) private information.

59. Defendants' failure to secure and protect Plaintiff's and Class Members' PCAI directly resulted in the public disclosure of such private information.

60. Dissemination of Plaintiff's and Class Members' PCAI is not of a legitimate public concern; publicity of their PCAI would be, is and will continue to be, offensive to Plaintiff, Class Members, and other reasonable people.

61. Plaintiff and the Class Members were (and continue to be) damaged as a direct and/or proximate result of Defendants' invasion of their privacy by publicly disclosing their private facts (*i.e.,* their PCAI) in the form of, *inter alia,* expenses for credit monitoring and

identity theft insurance, out-of-pocket expenses, anxiety, emotional distress, loss of privacy, and other economic and non-economic harm – for which they are entitled to compensation. At the very least, Plaintiff and the Class Members are entitled to nominal damages.

62. Defendants' wrongful actions and/or inaction (as described above) constituted (and continue to constitute) an invasion of Plaintiff's and Class Members' privacy by publicly disclosing their private facts (*i.e.,* their PCAI).

COUNT IV

NEGLIGENCE

63. Plaintiff repeats and re-alleges the allegations contained in the foregoing paragraphs as if fully set forth herein.

64. Defendants MAPCO and DELEK assumed a duty to use reasonable care to keep the credit card and other nonpublic information of the Class that is, or was, in its possession and control private and secure. By its acts and omissions described herein, Defendant unlawfully breached this duty. The Class was damaged thereby.

65. The private financial information of the Class that was compromised by the breach of Defendants' security included, without limitation, information that was being improperly stored and inadequately safeguarded in violation of, among other things, industry rules and regulations. Those rules and regulations created a duty of reasonable care and a standard of care that was breached by Defendant.

66. The breach of security was a direct and proximate result of Defendants' failure to use reasonable care to implement and maintain appropriate security procedures reasonably designed to protect the credit and debit card information and other nonpublic information of the

Class. This breach of security and unauthorized access to the private nonpublic information of the Class was reasonably foreseeable.

67. Defendant was in a special fiduciary relationship with the Class by reason of its entrustment with credit and debit card information and other nonpublic information. By reason of this fiduciary relationship, Defendant had a duty of care to use reasonable means to keep the credit and debit card information and other nonpublic information of the Class private and secure. Defendant also had a duty to inform the Class Members in a timely manner when their credit and debit card information and other nonpublic information became compromised. Defendant has unlawfully breached these duties.

68. Pursuant to Class Members' rights to privacy, Defendant had a duty to use reasonable care to prevent the unauthorized access, use, or dissemination of the credit and debit card information and other nonpublic information. Defendant unlawfully breached this duty.

69. The compromise of the Class' nonpublic information, and the resulting burden, fear, anxiety, emotional distress, loss of time spent seeking to prevent or undo any further harm, and other economic and non-economic damages to the Class, were the direct and proximate result of Defendants' violation of its duty of care.

70. Defendant had a duty to timely disclose the data compromise to all customers whose credit and debit card information and other nonpublic information was, or was reasonably believed to have been, accessed by unauthorized persons. Disclosure was required so that, among other things, the affected customers could take appropriate measures to avoid unauthorized charges on their accounts, cancel or change account numbers on the compromised cards, and monitor their account information and credit reports for fraudulent charges.

Defendant breached this duty by failing to notify Class Members in a timely manner that their information was compromised. Class Members were harmed by Defendants' delay because, among other things, fraudulent charges have been made to Class Members' accounts.

71. Defendant had a duty to use reasonable care to destroy, and not unnecessarily store, credit and debit card information and other personal information of the Class. By the acts described herein, Defendant negligently breached this duty, and the Class was harmed thereby.

72. Defendant had a duty to use a security system that would protect Class Members' credit and debit card information while that information is on the Defendants' network and to protect that information from being accessed by unauthorized third parties.

73. Defendant knew or should have known that its network for processing and storing credit and debit card transactions and related information had security vulnerabilities. Defendant was negligent in continuing such data processing in light of those vulnerabilities and the sensitivity of the data.

74. As a direct and proximate result of Defendants' conduct, the Class suffered damages including, but not limited to, loss of control of their credit card and other personal financial information; monetary loss for fraudulent charges incurred on their accounts; fear and apprehension of fraud, loss of money, and identify theft; the burden and cost of credit monitoring to monitor their accounts and credit history; the burden and cost of closing compromised accounts and opening new accounts; the burden of closely scrutinizing credit card statements for past and future transactions; damage to their credit history; loss of privacy; and other economic damages.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and all others similarly situated, respectfully requests the following relief:

A. That this Court certify this action as a Class action pursuant to Federal Rules of Civil Procedure 23(a) and (b)(3), and appoint Plaintiff and her counsel to represent the Class;

B. That this Court enter judgment in favor of Plaintiff and the Class, and against Defendants MAPCO and DELEK under the legal theories alleged herein;

C. That this Court award damages under the common law theories alleged herein;

D. That this Court award attorneys' fees, expenses, and costs of this suit;

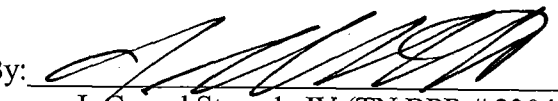
E. That this Court award Plaintiff and the Class pre-judgment and post-judgment interest at the maximum rate allowable by law; and

F. That this Court award such other and further relief as it may deem just and appropriate.

JURY TRIAL DEMAND

Plaintiff, on behalf of herself and the Class, demands a trial by jury on all issues so triable.

Date: August 20, 2014

By: 

J. Gerard Stranch, IV (TN BPR # 23045)
Benjamin A. Gastel (TN BPR # 28699)
BRANSTETTER, STRANCH & JENNINGS, PLLC
227 Second Avenue No., 4th Floor
Nashville, TN 37201-1631
Telephone: (615) 254-8801
gerards@branstetterlaw.com
beng@branstetterlaw.com

Joseph P. Guglielmo
SCOTT+SCOTT, Attorneys at Law, LLC
The Chrysler Building
405 Lexington Avenue, 40th Floor
New York, NY 10174
Telephone: (212) 223-4478
jguglielmo@scott-scott.com

Attorneys for Plaintiff